

Title (en)
PUBLIC KEY DIVERSIFICATION METHOD.

Title (de)
DIVERSIFIZIERUNGSVERFAHREN FÜR ÖFFENTLICHE SCHLÜSSEL.

Title (fr)
PROCEDE DE DIVERSIFICATION DE CLES PUBLIQUES.

Publication
EP 0400103 A1 19901205 (EN)

Application
EP 89909280 A 19890727

Priority
• GB 8819767 A 19880819
• US 36494989 A 19890612

Abstract (en)
[origin: WO9002456A1] A method is disclosed whereby individual members of a group of members or entities may be provided, under the control of a trusted member, referred to as the parent, with respective individual secret keys for use in public key cryptography, such that the matching public key can be readily derived, and group membership authenticated. The parent initially establishes a public key (e, N) where $N = P.Q$ is the product of two primes. In response to a request from a group member, the parent selects two further primes R, S and communicates two values dependent thereon to the requesting member, which selects two more primes T and U for use in conjunction with the received values to establish the member's secret key.

Abstract (fr)
On a mis au point un procédé selon lequel des personnes d'un groupe de membres ou d'entités se voient attribuées, sous la commande d'un membre investi de confiance, appelé le parent, des clés secrètes individuelles utilisées dans la cryptographie de clés publiques, de manière à pouvoir dériver facilement l'appariement de la clé publique, et authentifier la qualité de membre d'un groupe. Le parent établit initialement une clé publique (e, N), $N = P.Q$ étant le produit de deux nombres premiers. En réponse à une demande émanant d'un membre du groupe, le parent choisit deux autres nombres premiers R, S et communique deux valeurs dépendantes de ceux-ci au membre demandeur, qui choisit deux nombres premiers de plus T et U utilisés conjointement avec les valeurs reçues afin d'établir la clé secrète du membre.

IPC 1-7
H04L 9/30

IPC 8 full level
H04L 9/08 (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP)
H04L 9/302 (2013.01); **H04L 9/3249** (2013.01)

Citation (search report)
See references of WO 9002456A1

Designated contracting state (EPC)
CH DE FR GB LI NL

DOCDB simple family (publication)
WO 9002456 A1 19900308; AU 4052489 A 19900323; AU 607351 B2 19910228; DE 68907717 D1 19930826; DE 68907717 T2 19940217; EP 0400103 A1 19901205; EP 0400103 B1 19930721; JP H03505033 A 19911031

DOCDB simple family (application)
US 8903253 W 19890727; AU 4052489 A 19890727; DE 68907717 T 19890727; EP 89909280 A 19890727; JP 50865389 A 19890727